PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

CRIAÇÃO DE EQUIPES DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS - ETIR

ORIGEM

Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA

Art. 6º da Lei nº 10.683, de 28 de maio de 2003.
Art. 8º do Anexo I do Decreto nº 5.772, de 8 de maio de 2006.
Decreto nº 3.505, de 13 de junho de 2000.
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008.
Incisos II e IV do art. 37 da Portaria nº 13 do Gabinete de Segurança Institucional, de 4 de agosto de 2006.

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

2 CONSIDERAÇÕES INICIAIS

2.1 Nos últimos anos os órgãos públicos vêm implementando e consolidando redes locais de computadores cada vez mais amplas, como exigência para suportar o fluxo crescente de informações, bem como permitir que seus funcionários acessem à rede mundial de computadores para melhor desempenharem suas funções. Manter a segurança da informação e comunicações de uma organização em um ambiente computacional interconectado nos dias atuais é um grande desafio, que se torna mais difícil à medida que são lançados novos produtos para a Internet e novas ferramentas de ataque são desenvolvidas.

2.2 Diante da premissa de garantir e incrementar a segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta, há a necessidade de orientar a condução de políticas de segurança já existentes ou a serem implementadas.

2.3 Considerando a estratégia de segurança da informação composta por várias camadas, uma delas, que vem sendo adotada por diversas instituições, é a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais, mundialmente conhecido como CSIRT® (do inglês "Computer Security Incident Response Team").

2.4 É competência da Coordenação-Geral de Tratamento de Incidentes de Redes do Departamento de Segurança da Informação e Comunicações – DSIC do Gabinete de Segurança Institucional – GSI apoiar os órgãos e entidades da Administração Pública Federal, direta e indireta, nas atividades de capacitação e tratamento de incidentes de segurança em redes de computadores, conforme disposto nos incisos III e VI do art. 39 do anexo da Portaria nº 13 do GSI, de 04 de agosto de 2006.

2.5 É condição necessária para a criação de uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, o órgão ou entidade possuir a competência formal e respectiva atribuição de administrar a infra-estrutura da rede de computadores de sua organização.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações – DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

4.1 **Agente responsável:** Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

4.2 **Artefato malicioso**: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

4.3 **Comunidade ou Público Alvo**: é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

4.4 **CTIR GOV**: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações – DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI;

4.5 **Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR**: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

4.6 **Incidente de segurança**: é qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

4.7 **Serviço**: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

4.8 **Tratamento de Incidentes de Segurança em Redes Computacionais:** é o serviço que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências;

4.9 **Vulnerabilidade**: é qualquer fragilidade dos sistemas computacionais e redes de computadores que permitam a exploração maliciosa e acessos indesejáveis ou não autorizados.

5 RESPONSABILIDADE

Os Gestores de Segurança da Informação e Comunicações são os responsáveis por coordenar a instituição, implementação e manutenção da infraestrutura necessária às Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais, nos órgãos e entidades da Administração Pública Federal, direta e indireta, conforme descrito no inciso V do art 5º da Instrução Normativa nº 01, do Gabinete de Segurança Institucional, de 13 de junho de 2008.

6 DEFINIÇÃO DA MISSÃO

6.1 A missão deve fornecer uma breve e inequívoca descrição dos objetivos básicos e a função da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais. A definição da missão fornecerá a linha base para as atividades a serem desenvolvidas pela Equipe.

6.2 Recomenda-se como missão prioritária para a Equipe a facilitação e a coordenação das atividades de tratamento e resposta a incidentes em redes computacionais, além de alguma outra missão específica, em consonância com as atividades de resposta e tratamento a incidentes em redes, tais como: recuperação de sistemas, análise de ataques e intrusões, cooperação com outras equipes, participação em fóruns e redes nacionais e internacionais.

6.3 A definição da missão, juntamente com os serviços a serem prestados pela Equipe, influenciará o modelo de implementação mais adequado à necessidade da organização.

6.4 As missões da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais deverão ser descritas no respectivo documento de sua constituição, conforme o Anexo A desta Norma Complementar.

7 MODELO DE IMPLEMENTAÇÃO

Cada órgão ou entidade deverá estabelecer, dentre os modelos apresentados abaixo, aquele que melhor se adequar às suas necessidades e limitações, ressalvado que, independentemente do modelo escolhido, deverão ser observadas as diretrizes desta Norma Complementar. Nada obstante, em quaisquer dos modelos estabelecidos deverá ser designado formalmente o Agente Responsável, que terá, dentre outras atribuições, a de ser a interface com o Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV. Este Agente será o responsável por criar os procedimentos internos, gerenciar as atividades e distribuir tarefas para a Equipe ou Equipes que compõem a ETIR.

7.1 Modelo 1 – Utilizando a equipe de Tecnologia da Informação – TI

7.1.1 Neste modelo não existirá um grupo dedicado exclusivamente às funções de tratamento e resposta a incidentes de Rede. A Equipe será formada a partir dos membros das equipes de TI do próprio órgão ou entidade, que além de suas funções regulares passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes em redes computacionais. Neste modelo as funções e serviços de tratamento de incidente deverão ser realizadas, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos em segurança.

7.1.2 A Equipe que utilizar este modelo desempenhará suas atividades, via de regra, de forma reativa, sendo desejável, porém que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades pró-ativas.

7.2 Modelo 2 – Centralizado

7.2.1 A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais será estabelecida de forma centralizada no âmbito da organização.

7.2.2 A Equipe será composta por pessoal com dedicação exclusiva às atividades de tratamento e

resposta aos incidentes em redes computacionais.

7.3 Modelo 3 – Descentralizado

7.3.1 No modelo descentralizado a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais será composta por colaboradores distribuídos por diversos locais dentro da organização, dispersos por uma região ou pelo país inteiro. Essas equipes devem possuir pessoal próprio dedicado às atividades de tratamento e resposta aos incidentes de rede computacionais, podendo atuar operacionalmente de forma independente, porém alinhadas com as diretrizes estabelecidas pela coordenação central.

7.3.2 A ETIR da organização será formada pelo conjunto dessas equipes distribuídas e chefiada pelo Agente Responsável designado.

7.4 Modelo 4 – Combinado ou Misto

7.4.1 Trata-se da junção dos modelos Descentralizado e Centralizado. Neste modelo existirá uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais central e Equipes distribuídas pela organização.

7.4.2 A Equipe central será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as Equipes descentralizadas, além de ser a responsável, perante toda a organização, pela comunicação com o CTIR GOV.

7.4.3 As Equipes distribuídas serão responsáveis por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade.

8 ESTRUTURA ORGANIZACIONAL

8.1 Existem muitas maneiras diferentes de uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais ser estruturada. A estrutura dependerá do modelo de implementação a ser adotado, do tamanho da organização, do número de localizações geográficas distribuídas e onde as funções estão localizadas, do número de sistemas e plataformas suportadas, do número de serviços a serem oferecidos e do conhecimento técnico do pessoal existente.

8.2 Os membros da Equipe deverão ser selecionados, sempre que possível, dentre o pessoal existente, com perfil técnico adequado às funções de tratamento de incidentes de rede, os quais deverão dedicar o tempo integral, ou um percentual do seu tempo de trabalho, dependendo do modelo de implementação adotado, de forma reativa e pró-ativa.

8.3 O percentual do esforço dedicado será negociado entre a supervisão de cada um dos membros e o Agente Responsável pela Equipe e deverá estar descrito no documento de constituição da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

8.4 Recomenda-se que os membros da ETIR sejam: administradores de sistema ou de segurança, administradores de banco de dados, administradores de rede, analistas de suporte ou quaisquer outras pessoas da organização com conhecimento técnico comprovado. A Equipe poderá ser

estendida com a inclusão dos seguintes membros: representantes legais de áreas específicas da organização, advogados, estatísticos, recursos humanos, relações públicas, gestão de riscos, controle interno e grupo de investigação, ou outro que a organização entenda ser adequado.

8.5 Para cada membro da Equipe deverá ser designado um substituto que deverá ser treinado e orientado para a realização das tarefas e atividades da ETIR.

8.6 O Gestor de Segurança da Informação e Comunicações da organização será o responsável por prover os meios necessários para a capacitação e o aperfeiçoamento técnico dos membros da Equipe, bem como prover a infraestrutura necessária.

9 AUTONOMIA DA ETIR

A autonomia da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR descreve o escopo de atuação e o nível de responsabilidade que a Equipe tem sobre as suas próprias ações e sobre as atividades de resposta e tratamento dos incidentes na rede de computadores. A autonomia define o nível de controle da Equipe no relacionamento com os componentes da sua organização. A autonomia deverá ser definida, explicitamente, no documento de constituição da ETIR, conforme apresentado no Anexo A desta Norma.

9.1 Autonomia Completa

Se uma ETIR tem plena autonomia, ela poderá conduzir o seu público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança. Durante um incidente de segurança, se tal se justificar, a Equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

9.2 Autonomia Compartilhada

9.2.1 Se a ETIR possui a autonomia compartilhada, ela trabalhará em acordo com os outros setores da organização a fim de participar do processo de tomada de decisão sobre quais medidas devam ser adotadas.

9.2.2 A ETIR participará no resultado da decisão, sendo, no entanto, apenas um membro no processo decisório. Neste caso, a Equipe poderá recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque e discutirá as ações a serem tomadas (ou as repercussões se as recomendações não forem seguidas) com os outros membros da organização.

9.2.3 A indicação dos membros do processo decisório deverá ser definida explicitamente no documento de constituição da ETIR.

9.3 Sem Autonomia

9.3.1 Se uma Equipe não tem autonomia, só poderá agir com a autorização de um membro da organização com a autoridade para tal, designado no documento de constituição da ETIR.

9.3.2 A ETIR não terá autonomia para a tomada de decisões ou adoção de ações, podendo, no entanto, recomendar os procedimentos a serem executados ou as medidas de recuperação durante um ataque, mas não terá um voto na decisão final.

9.3.3 A ETIR poderá ser capaz, devido à sua posição na organização e capacidade técnica, de conduzir os tomadores de decisão a agir durante um incidente de segurança, ressalvado o caráter sugestivo das recomendações.

10 DISPOSIÇÕES GERAIS

10.1 Os órgãos ou entidades que inicialmente optarem pela implantação do Modelo 1 (Utilizando a equipe de Tecnologia da Informação) deverão, assim que possível, migrar para um dos outros modelos.

10.2 Preferencialmente a Equipe deve ser composta por servidores públicos ocupantes de cargo efetivo ou militares de carreira, conforme o caso, com perfil técnico compatível, lotados nos seus respectivos órgãos.

10.3 Cada órgão poderá deliberar o nome de sua Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

10.4 A ETIR deverá guiar-se por padrões e procedimentos técnicos e normativos no contexto de tratamento de incidentes de rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal – CTIR GOV.

10.5 A ETIR poderá usar as melhores práticas de mercado, desde que não conflitem com os dispositivos desta Norma Complementar.

10.6 A ETIR deverá comunicar de imediato a ocorrência de todos os incidentes de segurança ocorridos na sua área de atuação ao CTIR GOV, conforme padrão definido por esse órgão, a fim de permitir a geração de estatísticas e soluções integradas para a Administração Pública Federal.

10.7 A troca de informações e a forma de comunicação entre as ETIR, e entre estas e o CTIR GOV, serão formalizadas caso a caso, se necessário, por Termo de Cooperação Técnica.

11 VIGÊNCIA

Esta Norma Complementar entra em vigor na data de sua publicação.

12 ANEXO

A – DOCUMENTO DE CONSTITUIÇÃO DA ETIR.

ANEXO A

DOCUMENTO DE CONSTITUIÇÃO DA ETIR

A fim de regulamentar o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR, os órgãos e entidades da Administração Pública Federal, direta e indireta – APF deverão elaborar e publicar o Documento de Constituição da ETIR, alinhado com a Política de Segurança da Informação e Comunicações, devidamente aprovado pela Alta Administração do órgão ou entidade.
No documento de constituição da ETIR deverão constar, no mínimo, os seguintes pontos: definição da missão, comunidade ou público alvo, modelo de implementação escolhido, estrutura organizacional, autonomia e serviços que serão prestados.

1 MISSÃO

A missão deve fornecer uma breve e inequívoca descrição dos objetivos básicos e a função da ETIR. A organização deve observar o previsto no item 6 desta Norma Complementar e as seguintes premissas no que se refere à definição da missão:

1.1 Não deve conter termos ambíguos;

1.2 Não deve ser extensa, descrevendo de forma sucinta a missão da ETIR;

1.3 Deve ajudar a Equipe a entender os seus objetivos;

1.4 Deve complementar a missão do órgão ao qual pertence;

1.5 Deve estar alinhada à Política de Segurança da Informação e Comunicações do órgão ou entidade.

2 COMUNIDADE OU PÚBLICO ALVO

2.1 Deve ser formada pelos usuários da rede de computadores e sistemas do(s) órgão(ãos) ou entidade(s) atendidos pela ETIR.

2.2 Deve ser descrito o público com o qual a Equipe irá se relacionar, principalmente quando este não for composto por todos os integrantes do próprio órgão ou entidade, além da forma e as condições nas quais a comunicação será realizada.

2.3 Devem ser descritos ainda os relacionamentos com outros organismos de tratamento de incidente e as condições deste relacionamento.

3 MODELO DE IMPLEMENTAÇÃO

Cada órgão ou entidade deve estabelecer o modelo que melhor se adequar às suas necessidades e limitações, dentre os apresentados no item 7 desta Norma Complementar, descrevendo o modelo de forma detalhada e a maneira de atuação da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais dentro da organização.

4 ESTRUTURA ORGANIZACIONAL

Observadas as diretrizes constantes no item 8 desta Norma Complementar, deve ser definida a estrutura organizacional da ETIR, nos seguintes termos:

4.1 Posição na estrutura organizacional do órgão a que pertence;

4.2 Definição do Agente Responsável pela ETIR, suas competências, atribuições e responsabilidades perante o Gestor de Segurança da Informação e Comunicações, as demais esferas decisórias da organização e o CTIR GOV;

4.3 Definição da Equipe e/ou Equipes descentralizadas, seus membros componentes e membros agregados, suas funções, responsabilidades, maneira de atuação e tempo destinado às tarefas da ETIR;

4.4 Definição dos membros substitutos, suas atribuições e responsabilidades.

5 AUTONOMIA DA ETIR

5.1 Na definição da autonomia da ETIR o órgão ou entidade deve observar as diretrizes constantes no item 9 desta Norma Complementar.

5.2 Devem ser definidos explicitamente o modelo adotado, o escopo de atuação, o nível de responsabilidade e a independência da Equipe sobre as ações necessárias à resposta e tratamento dos incidentes de segurança na rede de computadores, divulgando para toda a organização.

5.3 Dependendo do nível de autonomia da ETIR, devem ser indicados os membros da organização com autoridade para decidir sobre as ações a serem adotadas.

6 SERVIÇOS

6.1 Para a definição dos serviços que serão prestados cada órgão deve observar as suas necessidades e limitações, a missão, o modelo de implementação adotado e a autonomia da ETIR, tudo em consonância com o que prescreve esta Norma Complementar.

6.2 Os serviços prestados por uma ETIR definem quais os procedimentos a Equipe desempenhará. Para cada serviço este documento deve descrever, no mínimo, os seguintes atributos:

6.2.1 Objetivo;

6.2.2 Definição;

6.2.3 Descrição das funções e procedimentos que compõem o serviço;

6.2.4 Disponibilidade do serviço: quando, como e onde o serviço será oferecido;

6.2.5 Metodologia para execução do serviço.

6.3 A ETIR deve implementar, no mínimo, o serviço de Tratamento de Incidentes de Segurança em Redes Computacionais. Este serviço, conforme sua definição, consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

6.4 A Equipe poderá oferecer à sua comunidade ou público alvo, além do tratamento de incidentes, outros serviços correlacionados à resposta e tratamento de incidentes de segurança em redes computacionais, de acordo com normas nacionais e internacionais.